UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/851,625	05/08/2001	Rajasekhar Sistla	P10212	3678

50890 7590 05/25/2010
Caven & Aghevli LLC
c/o CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER	
TRUONG, LAN DAI T	
ART UNIT	**PAPER NUMBER**
2452	

MAIL DATE	DELIVERY MODE
05/25/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/851,625	**Applicant(s)** SISTLA, RAJASEKHAR	
	Examiner LAN-DAI Thi TRUONG	**Art Unit** 2452	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01/22/2010* .

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is response to communications: application, filed on 05/08/2001; amendments filed on 01/22/2010. Claims 1-21 are pending; claims 1, 6, 11, 17 are amended.

2. Applicant's arguments/ amendments filed on 01/22/2010 have been fully considered, but are moot in view of the new ground(s) of rejection.

Claim Objection

3. Claims 6, 11 and 17 are objected to because of the following informalities: Those are indicated as 'Previously Presented' statuses; however, they are amended. Appropriate corrections are required.

Claim rejections-35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-21 are rejected under 35 U.S.C 103(a) as being un-patentable over Kobata et al. (U.S. 2003/0023695) in view of Gupta el al. (2007/0016647) and further in view of Spraggs (U.S. 6,941,454).

Regarding claim 1:

Kobata discloses the invention substantially as claimed, including a method, which can be implemented in a computer hardware or software code for preserving confidentiality of an electronic mail from a sender to a recipient, the method comprising:

restricting the recipient's ability to modify contents of the electronic mail based on a confidentiality level established by the sender, wherein a user interface is to comprise a first set of confidentiality levels from which the sender is to select: (a user interface comprise a set of selectable functions (i.e. “send secure;” “preventing forwarding;” “preventing copy” …etc.), wherein the sender could set restrictions options for recipient's ability to modify receiving content: Kobata, [0220]; figures 26 & 28; [0215]).

However, Kobata does not explicitly disclose from a mail server, restricting to modify electronic mail or authenticating identity information based on data provided by an authentication server.

In analogous art, Gupta discloses an collaboration email system comprises communicative connections between email clients and mail servers; wherein one of email client is capable to create collaborative email message and select process preferences for that collaborative message (e.g. restricting recipient to modify email), so that based on those selected preferences the mail server will process the collaborative email message, see ([0065]; [0099]; [0101]-[0102]; [0107]).

authenticating identity information provided by an authentication server: (receiving authentication information from an authentication authority: Gupta: [0130]; figure 4) (where, “authentication authority” reads on ' authentication server’ as claimed).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Gupta's ideas of providing email client capability of selecting email process preferences (e.g. restricting recipient to modify email), so that based on those selected preferences the mail server will process the email into Kobata's system in order to provide an efficient collaboration communication system (e.g. providing server system supporting collaborative messaging based on electronic email), see (Gupta, [0006]).

However, Kobata-Gupta does not explicitly disclose encrypting the electronic mail, at the recipient, with the authenticated identity information if the recipient attempts to store the electronic mail to a local storage.

In analogous art, Spraggs discloses a server is capable to re-encrypt the decrypted data those are received from a sending client with the server key and store the re-encrypted data into a secure database, see (Spraggs, column 3, lines 45-51).

decrypting the electronic mail, at the recipient if the recipient attempts to retrieve the electronic mail from the local storage: (Spraggs further discloses the server decrypts the stored re-encrypted data when it attempts to retrieve the data from the secure database responsive to client requests, see (Spraggs, column 3, lines 45-67).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Spraggs's ideas of providing a server capability of re-encrypting data prior storing them into a secure database into Kobata-Gupta's system in order to provide higher secure level communication system, see (Spraggs, column 1, lines 44-47).

Regarding claim 2:

In addition to rejection in claim 1, Kobata- Gupta-Spraggs further discloses wherein the identity information is a system password: (providing user IDs and Passwords for authentication process: Kobata, [0070]).

Regarding claim 3:

In addition to rejection in claim 1, Kobata- Gupta-Spraggs further discloses prompting a user of the recipient to supply the identity information: (a receiver is requested to provide user IDs and Passwords for authentication process: Kobata, [0070]).

decrypting the electronic mail with the identity information supplied by the user: (In Spraggs's system, the receiving client can decrypt data via using it's private key: column 3, lines 65-67).

Regarding claim 4:

In addition to rejection in claim 1, Kobata- Gupta-Spraggs further discloses asserting a control signal to disable options that are originally supported by the recipient if the confidentiality level satisfies a predefined confidentiality threshold: (restrictions options for recipient's ability to modify receiving content: Kobata, [0220]; figures 26 & 28; [0215]).

Regarding claim 5:

In addition to rejection in claim 4, Kobata- Gupta-Spraggs further discloses the control signal is a control signal: (Kobata, [0220]; figures 26 & 28; [0215]).

Regarding claim 6:

Kobata discloses the invention substantially as claimed, including an electronic mail confidentiality preserver of a recipient email client, which can be implemented in a computer hardware or software code, comprising:

an input-processing engine to limit abilities of a user of the recipient email client to modify contents of an electronic mail received by the recipient email client based on a confidentiality level, wherein a user interface further comprises a first set of confidentiality levels from which a user of a sender email client is to select irrespective of the recipient's email address: (a user interface comprise a set of selectable functions (i.e. “send secure;” “preventing forwarding;” “preventing copy”; “receiving address"....etc.), wherein the sender could set restrictions options for recipient's ability to modify receiving content: Kobata, [0220]; [0221]; figures 26; figure 28; figure 29; figure 30; [0215]).

However, Kobata does not explicitly disclose from a mail server, limiting to modify electronic mail.

In analogous art, Gupta discloses an collaboration email system comprises communicative connections between email clients and mail servers; wherein one of email client is capable to create collaborative email message and select process preferences for that collaborative message (e.g. restricting recipient to modify email), so that based on those selected preferences the mail server will process the collaborative email message, see ([0065]; [0099]; [0101]-[0102]; [0107]).

authenticating identity information provided by an authentication server: (receiving authentication information from an authentication authority: Gupta: [0130]; figure 4) (where, “authentication authority” reads on ' authentication server’ as claimed).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Gupta's ideas of providing email client capability of selecting email process preferences (e.g. restricting recipient to modify email), so that based on those selected preferences the mail server will process the email into Kobata's system in order to provide efficient collaboration communication system (e.g. providing server system supporting collaborative messaging based on electronic email), see (Gupta, [0006]).

However, Kobata-Gupta does not explicitly disclose an encryption/decryption engine, coupled to the input-processing engine, to encrypt the electronic mail with authenticated identity information if the recipient attempts to store the electronic mail to a local storage.

In analogous art, Spraggs discloses a server is capable to re-encrypt the decrypted data those are received from a sending client with the server key and store the re-encrypted data into a secure database, see (Spraggs, column 3, lines 45-51).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Spraggs's ideas of providing a server capability of re-encrypting data prior storing them into a secure database into Kobata-Gupta's system in order to provide higher secure level communication system, see (Spraggs, column 1, lines 44-47).

Regarding claim 7:

This claim is rejected under rationale of claim 4.

Regarding claim 8:

This claim is rejected under rationale of claim 5.

Regarding claim 9:

In addition to rejection in claim 6, Kobata-Gupta-Spraggs further discloses the input processing engine further asserts a second control signal to invoke the encryption/decryption engine in response to the user's access: (Spraggs: column 3, lines 65-67; column 4, lines 1-2).

Regarding claim 10:

In addition to rejection in claim 6, Kobata-Gupta-Spraggs further discloses prompting the user for identity information: (Spraggs: figure 7, items 710, 712).

decrypting the electronic email with the identity information: (Spraggs: figure 7, items 710, 712).

encrypts the electronic mail with the identity information to store the electronic mail: (Spraggs: figure 7, item 708; column 3, lines 45-51).

decrypts the electronic mail to retrieve the electronic mail: (the receiving client can decrypt data via using it's private key: Spraggs: column 3, lines 65-67).

Regarding claim 11:

Kobata discloses the invention substantially as claimed, including a electronic mail clients, comprising:

a user interface: (Kobata: figure 26).

a communication engine: (a communication engine should be inherently included in Kobata’s system: Kobata: figure 26).

a local storage: (a storage for storing folders/ files: Kobata, figure 22D).

and an electronic mail confidentiality preserver (email server: Kobata, figure 17, item 1715) , coupled to the user interface (Kobata: figure 26), coupled to the communication engine

(Kobata: figure 26) and coupled to the local storage (a storage for storing folders/ files: Kobata, figure 22D), wherein the electronic mail confidentiality preserver further comprises:

an input-processing engine to limit abilities of a user of the recipient email client to modify contents of an electronic mail received by the recipient email client based on a user-selected confidentiality level; wherein the user interface further comprises a first set of confidentiality levels from which a user is to select: (a user interface comprise a set of selectable functions (i.e. “send secure;” “preventing forwarding;” “preventing copy”; “receiving address"....etc.), wherein the sender could set restrictions options for recipient's ability to modify receiving content: Kobata, [0220]; [0221]; figures 26; figure 28; figure 29; figure 30; [0215]).

However, Kobata does not explicitly disclose from a mail server, limiting to modify electronic mail.

In analogous art, Gupta discloses an collaboration email system comprises communicative connections between email clients and mail servers; wherein one of email client is capable to create collaborative email message and select process preferences for that collaborative message (e.g. restricting recipient to modify email), so that based on those selected preferences the mail server will process the collaborative email message, see ([0065]; [0099]; [0101]-[0102]; [0107]).

authenticating identity information provided by an authentication server: (receiving authentication information from an authentication authority: Gupta: [0130]; figure 4) (where, “authentication authority” reads on ' authentication server’ as claimed).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Gupta’s ideas of providing email client capability of selecting email process preferences (e.g. restricting recipient to modify email), so that based on those selected preferences the mail server will process the email into Kobata's system in order to provide efficient collaboration communication system (e.g. providing server system supporting collaborative messaging based on electronic email), see (Gupta, [0006]).

However, Kobata-Gupta does not expliclity disclose an encryption/decryption engine, coupled to the input-processing engine, to encrypt the electronic mail with authenticated identity information if the recipient attempts to store the electronic mail to a local storage.

In comparable art, Spraggs discloses a server is capable to re-encrypt the decrypted data those are received from a sending client with the server key and store the re-encrypted data into a secure database, see (Spraggs, column 3, lines 45-51).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Spraggs's ideas of providing a server capability of re-encrypting data prior storing them into a secure database into Kobata-Gupta's system in order to provide higher secure level communication system, see (Spraggs, column 1, lines 44-47).

Regarding claim 12:

In addition to rejection in claim 11, Kobata-Gupta-Spraggs further discloses wherein the user interface further comprises a second set of options to manipulate the electronic mail from which the user is to select: (a user interface comprise a set of selectable functions (i.e. "send secure;" "preventing forwarding;" "preventing copy"; "receiving address"....etc.), wherein the sender could set restrictions options for recipient's ability to modify receiving content: Kobata, [0220]; [0221]; figures 26; figure 28; figure 29; figure 30; [0215]).

Regarding claim 13:

In addition to rejection in claim 12, Kobata-Gupta-Spraggs further discloses asserting a control signal to disable options that are originally supported by the recipient if the confidentiality level satisfies a predefined confidentiality threshold: (restrictions options for recipient's ability to modify receiving content: Kobata, [0220]; figures 26 & 28; [0215]).

Regarding claim 14:

In addition to rejection in claim 13, Kobata-Gupta-Spraggs further discloses the control signal is a control signal: (Kobata, [0220]; figures 26 & 28; [0215]).

Regarding claim 15:

In addition to rejection in claim 12, Kobata-Gupta-Spraggs further discloses the input processing engine further asserts a second control signal to invoke the encryption/decryption engine in response to the user's access: (Spraggs: column 3, lines 65-67; column 4, lines 1-2).

Regarding claim 16:

In addition to rejection in claim 12, Kobata-Gupta-Spraggs further discloses prompting the user for identity information: (Spraggs: figure 7, items 710, 712).

decrypting the electronic email with the identity information: (Spraggs: figure 7, items 710, 712).

encrypts the electronic mail with the identity information to store the electronic mail: (Spraggs: figure 7, item 708; column 3, lines 45-51).

decrypts the electronic mail to retrieve the electronic mail: (the receiving client can decrypt data via using it's private key: Spraggs: column 3, lines 65-67).

Regarding claim 17:

Kobata discloses the invention substantially as claimed, including a storage device including a plurality of instructions readable therefrom, the instructions, when executed by a computer system, cause the computer system to perform operations comprising:

authenticating identity information of a recipient of an electronic mail: (authenticating identity information for recipient users: Kobata, [0173]-[0175]).

restricting the recipient's ability to modify contents of the electronic mail based on a confidentiality level established by a sender of the electronic mail, wherein a user interface is to comprise a first set of confidentiality levels from which the sender is to select: (a user interface comprise a set of selectable functions (i.e. "send secure;" "preventing forwarding;" "preventing copy" …etc.), wherein the sender could set restrictions options for recipient's ability to modify receiving content: Kobata, [0220]; figures 26 & 28; [0215]).

However, Kobata does not explicitly disclose from a mail server, restricting to modify electronic mail.

In analogous art, Gupta discloses an collaboration email system comprises communicative connections between email clients and mail servers; wherein one of email client is capable to create collaborative email message and select process preferences for that collaborative message (e.g. restricting recipient to modify email), so that based on those selected preferences the mail server will process the collaborative email message, see ([0065]; [0099]; [0101]-[0102]; [0107]).

authenticating identity information provided by an authentication server: (receiving authentication information from an authentication authority: Gupta: [0130]; figure 4) (where, “authentication authority” reads on ' authentication server’ as claimed).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Gupta’s ideas of providing email client capability of selecting email process preferences (e.g. restricting recipient to modify email), so that based on those selected preferences the mail server will process the email into Kobata’s system in order to provide efficient collaboration communication system (e.g. providing server system supporting collaborative messaging based on electronic email), see (Gupta, [0006]).

However, Kobata-Gupta does not explicitly disclose encrypting the electronic mail with the authenticated identity information if the recipient attempts to store the electronic mail to a local storage.

In comparable art, Spraggs discloses a server is capable to re-encrypt the decrypted data those are received from a sending client with the server key and store the re-encrypted data into a secure database, see (Spraggs, column 3, lines 45-51).

decrypting the electronic mail if the recipient attempts to retrieve the electronic mail from the local storage: (Spraggs further discloses the server decrypts the stored re-encrypted data when it attempts to retrieve the data from the secure database responsive to client requests, see (Spraggs, column 3, lines 45-67).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Spraggs’s ideas of providing a server capability of re-encrypting data prior storing them into a secure database into Kobata- Gupta's system in order to provide higher secure level communication system, see (Spraggs, column 1, lines 44-47).

Regarding claim 18:

This claim is rejected under rationale of claim 2.

Regarding claim 19:

This claim is rejected under rationale of claim 3.

Regarding claim 20:

This claim is rejected under rationale of claim 4.

Regarding claim 21:

This claim is rejected under rationale of claim 5.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Conclusions

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LAN-DAI Thi TRUONG whose telephone number is (571)272-7959. The examiner can normally be reached on Monday- Friday from 8:30am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thu Nguyen can be reached on 571-272-6967. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Patent Examiner
Ldt.
05/05/2010.

/DOHM CHANKONG/
Primary Examiner, Art Unit 2452